11   FISCAL/EQUIPMENT MANAGEMENT   *Effective: 11/01/02*
11.11 Security of WIC Data   *Revised: 06/01/06*

POLICY: Due to the confidentiality of the data maintained by the WIC ROSIE system, the local WIC Director must ensure that the data is secure and that access is restricted to only people authorized by WIC.

PROCEDURE:

A. SECURITY

1. Local Project Administrator

    a) Each local Project or Agency Director will designate a Local Project Administrator for ROSIE system administration. Larger Projects may want to designate a back-up Local Project Administrator.

    b) The Local Project Administrator will administer all user accounts for their project including creating new accounts for their project staff, unlocking accounts, resetting accounts to default passwords, modifying group access, modifying clinic access and inactivating accounts when a user is no longer working at that WIC project. In addition, Local Project Administrators will be able to update Project, Clinic and all Contact Information reported for each project.

    c) If a USER ID is needed and the Local Project Administrator is not available or there is not yet a Local Project Administrator designated, the request will need to be made to the State Office Administrator from either the Regional Nutritionist for the project or the Local Agency Director.

2. ROSIE User Security and Confidentiality Agreement

    a) The Local Project Administrator will implement and sign the User Security and Confidentiality Agreement, return the signed Agreement to the State WIC Office, and retain a copy at the Local Project.

    b) The Local Project Administrator is responsible to ensure all ROSIE users have read appropriate policies and have signed the User Security and Confidentiality Agreement. Copies of the Agreement can be found in WICPRO. The Local Project Administrator(s) will keep the signed agreements on file at the project. The signed agreement will cover project staff for their access to WIC Data and for those project staff that get access to the Ad-Hoc database.

3. ROSIE User ID

   a) Each user of ROSIE is required to have a unique USER ID. The ID will be created by the Local Project administrator or State Office Administrator; not the CIBER HelpDesk.

   b) The USER ID and password should not be shared with anyone and USER ID's should not be shared by WIC staff. Generic accounts should not be created; each account will have a designated user and only one user per account.

   c) User IDs in ROSIE must be inactivated when the employee leaves the WIC Agency. Project Directors must assure that within two weeks of an employee departure, their USER ID is inactivated in the system. The ID can be inactivated by the Local Project Administrator or the State Office Administrator.

   d) A password change will be forced every ninety (90) days by ROSIE.

4. All WIC data, whether in ROSIE or in Ad-Hoc tables, are subject to WIC confidentiality and security requirements.

5. WIC staff must exit out of the ROSIE website or remote program whenever the computer is not attended by a WIC staff member

6. A Screen Saver must be used on all WIC computers. This screen saver will have an assigned password that will go into effect after 10 minutes of keyboard/mouse inactivity.

B. REMOTE BACK-UP

1. For projects that have a remote site, where they do not have internet access, there is a remote capability within ROSIE. This is the only situation that requires back-ups to be performed by the local projects.

2. The back-up will occur on the machine that houses the ROSIE Synchronization icon. At remote sites, this machine acts as the server and holds a copy of the database locally. Instructions were provided by the State WIC Office during ROSIE roll-out on how to perform CD backups of the database.